Final Report

MobilePass

A secure, modular and distributed mobile border control solution for European land border crossing points

Grant agreement no. 608016

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

Project Data

Project Reference:	Grant agreement no. 608016
Project Short Name:	MobilePass
Project Name:	A secure, modular and distributed mobile border control solution for European land border crossing points
Call:	FP7-SEC-2013-3-2-3
Funding Scheme:	Capacity Project
Project web-site:	www.mobilepass-project.eu
Project Period	1.5.2015 – 31.12.2017
Confidentiality Status:	Publishable Summary
Project Partners:	- AUSTRIAN INSTITUTE OF TECHNOLOGY - AIT GmbH, Austria - FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V , Germany - UNIVERSITEIT MAASTRICHT UM-MERIT, Netherlands - REGULA BALTIJA SIA REGULA, Latvia - VIDEMO INTELLIGENTE VIDEOANALYSE GMBH & CO KG Videmo Germany - UNIVERSIDAD CARLOS III DE MADRID UC3M Spain - ITTI SP ZOO ITTI Poland - VERIDOS GMBH VERIDOS, Germany - INDRA SISTEMAS S.A. INDRA, Spain - INSPECTORATUL GENERAL AL POLITIEI DE FRONTIERA RBP Romania - MINISTERIO DEL INTERIOR MIR-DGP, Spain

Authors	**Name**	**Organization/Unit**
Main Author	Bernhard Strobl	AIT
Tel.:	+43 664 815 78 42	
Mail:	bernhard.strobl@ait.ac.at	MobilePassCoordinator@ait.ac.at
Contributing Author(s)	All WP Leaders	Different Project Partners

Authorization	**Name**	**Organization/Unit**
Project Officer	Agnieszka Marciniak	EC, REA
File	Final Report.docx	

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

Table of Content

1. Executive Summary

Promoting both security and mobility within the EU Border control is a major challenge for member states border control authorities. Travellers request a minimum delay and a convenient, non-intrusive border crossing, while border guards must fulfil their obligation to secure the EUs borders against illegal immigration, terrorisms, crime and other threats.

MobilePass focused on research and development towards technologically advanced mobile equipment at land border crossing points. The aim of the project is to provide new technologies for practical mobile devices which allow border control authorities to check European, visa-holding and frequent third country travellers in a comfortable, fast and secure way. The mobile solution incorporates new technologies needed in mobile scenarios and embeds them in the actual border crossing workflow to speed up control procedures.

MobilePass brought together system- and component producers, research institutions and governmental authorities. The entire innovation process, from components development to the integration into an efficient workflow was continuously evaluated by border guard authorities.

The MobilePass development process addressed both requirements with equal emphasis, kept security at the highest level while increasing the speed and the comfort for all legitimate travellers at land border crossing points. Aspects of a fast border crossing by legitimate travellers are

- a reliable and convenient capture of biometric and passport data
- dependable, secure wireless data transfer,
- and a modular mobile equipment optimized to the border control workflow.

Improved traveller identification technologies, such as **contactless fingerprint capture** and **advanced mobile facial capture** increase the security, minimise spoofing and evasion, while making the control less cumbersome for passengers.

A system evaluation and demonstration was done in two different member states. Compliance with European societal values and citizens' rights is central to the acceptance of the developed technologies, and will accompany the development throughout the project.

MobilePass developed technological advanced mobile equipment for border control authorities. The MobilePass approaches are advanced in technology beyond state-of-the-art in:

- Contactless multiple fingerprint verification
- Cooperative and fast face capturing and verification
- Full-page e-Passport scanning
- Communication reliability, security and speed
- Respect legal, ethical and social factors

The consortium carried out research and prototype development of electronics and algorithms embedded in a trusted platform module with secure boot mechanisms. Technological advances will bring a benefit for all general identity checks with legal ID Documents which can be read by a machine. This can be future Schengen Visa systems or personal ID cards combined with biometric features. Maximum attention is paid to the security features of these technologies. Research also included the development of a trusted platform computing module which will not allow re-engineering or compromising the build-in software in case of a stolen device.

The MobilePass consortium was fully aware that border management as such, as well as the specific research and technologies proposed within the MobilePass project are ethically sensitive. The consortium clearly states that it fully accepts and respects the ethical rules and standards of FP7, as well as those stated in the Charter of Fundamental Rights of the European Union incorporating experiences from border guards as well as feedback from passengers during the design phase.

To ensure this, the project output was screened by an internal and additional ethics and security committee.

All Information is also available on the MobilePass Website:
http://www.MobilePass-project.eu

2. Project context and the objectives

MobilePass identified and addressed 5 challenges which are described in the following sections:

1.1.1 Design, development and demonstration of a distributed and modular mobile border control solution based on the requirements and lessons learned of border control agencies

Current handheld devices for border control have the following disadvantages:

1. **Data Privacy Issues**: Compact handheld devices with integrated display may reveal sensitive information during the control process to other persons, when the device is handed over. Therefore, a modularity, separation and distribution of device components are envisaged.
2. **Data Security Issues**: theft and pilferage of such a device is a severe issue because onboard stored certificates e.g. for reading the RFID information are lost. Secure data architectures, encryption and remote data handling shall increase the security.
3. **Ergonomic aspects**: handling and lifting an integrated device (e.g. 1 kg) by security personal several thousand times a day leads to an antipathy using such devices. Also, some travellers do not interfere nicely with unknown mobile devices. The ergonomic aspect will be considered already in the design phase and the distributed concept will support the handling of the devices.
4. **Upgradability**: manufacturers of integrated devices tried to do their best in using latest technologies but new developments (e.g. contactless fingerprint readers) are complex to integrate, which needs time and slows the innovation process for emerging technologies. Also that upgrading process shall not compromise the security of the device and/or the process. The modularity concept as described will also contribute to allow upgradability.
5. **Communication Speed**: technological advances in cell phone communication are driven by the consumer industry and are fast. 3G/4G developments for data transmission speed have direct impact in passenger throughput. For a display/checking device which also handles the radio communication and shelters the user interface against a damage or erroneous, any future handheld device will be equipped with latest and fastest transmission technology.
6. **Tailoring**: Different countries have different demands in terms of device assembly, battery lifetime, operating temperatures and/or workflow management. A distributed solution will allow a tailor-made system. Additional requirements should be included fast and easily by 3rd parties.

With development of **modular and distributed concept** for advanced devices border control authorities will keep the central terminal with all sensitive information (only visible to the officer) in their proximity. A **second component** - which can be handed over to the traveller - will collect biometric and passport data.

The concept of a distributed, modular border control solution poses additional challenges that will be addressed by MobilePass:

- **Security if device lost** (storage of encryption keys, denial of service in case of loss of connection, no permanent storage of valuable information, countermeasures against re-engineering)
- **Resilience against** fraud, eavesdropping, spoofing, denial of service
- **Secure, reliable and fast wireless communication** between devices
- **Powerful embedded biometrics hardware design**

MobilePass solution for a distributed system will be

- **smaller** in terms of form factor comparing to existing solutions
- **more functional:** full page IR&UV passport scanner, contactless scanning of several fingers
- **faster:** simultaneous operation of different devices, newest cell-phone transmission
- **more secure**: no sensitive data stored in capturing devices, usage of encrypted wireless connection
- **more flexible** in terms of connection: any PC, handheld or smart phone, device interoperability
- **adaptable** for different scenarios thanks to a distributed approach

1.1.2 Design, development and evaluation of an embedded full-page passport scanner.

Available passport-reader provides the mandatory data of the MRZ and the check of some basic security features. This challenge is already well defined (a specified MRZ read by OCR). These devices have operational restrictions: they can guarantee verification of eDocuments only if this device is connected to PKD and has certificates for chip authentication. There is no chance to check optical security features of a document, since there is no full page scanning with IR or UV lights. As a conclusion, this type of device can be regarded as a registration device only. A full page optical reader will allow for verification of a document in case the RFID chip cannot be checked.

In future, optical inspection of the VIZ (visible inspection zone) with more different optical security features is an essential component which should be taken into account. MobilePass will investigate technical opportunities and develop a solution for a mobile/handheld ePassport scanner to inspect the security-features in the digital scanned images (colour, Infrared and UV) of a passport's datasheet. The developed solution should

- scan full page passports

- able to be handled by mobile personal (weight, ease of use, battery operated)
- connected wireless for easy handling (secure encrypted transmission)
- fast for maximizing passenger throughput
- secure against eavesdropping, spoofing and denial of service

1.1.3 Design, development and demonstration of a robust handheld contactless finger print scanner

Available fingerprint readers have several important disadvantages. One of the most important disadvantages in terms of performance and user acceptance is the need to have contact with the person's finger(s). Users of such systems have to fight against dropping performance due to the nature of the human finger: sweat, dirt and the antipathy of some people to put their finger(s) on a plate where millions others have done this before. In addition, there are security restrictions: to operate this device an officer has to handle a complete unit with display (which should not be seen by the person which is checked) and all sensitive data to a person in question, for example, in order to scan a fingerprint.

A radical new approach would be necessary to ease the use of biometric fingerprint scanning. Latest results in contactless fingerprint reading through application of structured light and a miniature camera seem to be a solution. MobilePass will investigate technical opportunities and develop a solution for a mobile fingerprint scanner, the solution should

- contactless operation
- fingerprint capture quality display
- able to be handled by mobile personal (weight, ease of use, battery operated)
- connected wireless for easy handling (secure encrypted transmission)
- fast for maximizing passenger throughput
- secure against eavesdropping, spoofing and denial of service
- robust against ambient conditions, especially light, temperature and humidity, as well as vibration due to the lack of a surface to lay down the device.

1.1.4 Design, development and demonstration of a fast, dedicated device for mobile face recognition

There are lots of mobile cameras available in mobile devices. In combination with operating system software and special image and video analytics, such integrated camera systems can be used for visual face verification.

However, camera systems integrated in such mobile devices (e.g. smart phones) are mainly designed for photographing every-day objects, by non-professionals. Hereby, the whole setup and workflow is optimized for generation of "good-looking snapshots", regardless of any possible automated post-processing of the camera data. As a first example, illumination conditions are “ignored” in a sense, that the camera is adapting to local illumination conditions to optimize the overall image for the user’s impression. In most cases, this is counterproductive for automated video analytics (e.g. automatic gain control, longer shutter period for lower noise, which causes motion blurring, etc.).

Further examples are manual focus adjustment, video capture capability for video (instead of only image) processing, integration of special active illumination (NIR), etc. Such features are not available or supported by today’s off-the-shelf mobile devices.

In MobilePass, a camera system optimized for the workflow in border control situations will be designed and exemplarily integrated. In contrary to standard mobile devices, the whole camera system, image/video capture and image pre-processing chain will focus on optimal conditions for later semi- or fully-automated face verification algorithms. The research on the envisioned solution will focus on

- designed of a single compact device
- video analytics for face detection, image enhancement and illumination compensation (for handling of challenging illumination conditions and camera ego-motion)
- multi-frame (video) processing for best-image-selection and multi-image fusion for de-noising and de-blurring
- automated quality estimation of captured face image and user feedback interactive control
- Integration of state-of-the-art face verification algorithms on mobile device, and performance evaluation

1.1.5 Design, development and demonstration of a flexible, reliable, and secure communication subsystem

Mobile data transmission is properly working in consumer applications like mobile internet or similar. When it comes to security critical systems, data transmission subsystems often work unsatisfactory and or even cannot deliver reliable connections.

One reason is that data transmission subsystem can be based on different types of network and also different privacy and security level. For the usage of public networks, the confidential level remains unknown because even if the radio transmission is ciphered, the access to databases via backhaul and backbone networks can be unprotected. The selection of the employed available network should be based on several aspects - most important is the security of data.

Moreover, the face verification generates a considerable volume of data that should be transmitted via broadband networks in order to decrease the time for the response.

Collocation problems related to radio equipment may be a source of radio interferences and limited network coverage.

The same requirements relate to the short-distance network that aggregates traffic from remote readers/scanners. Moreover this network should have enough capacity to accommodate the increasing number of these remote acquisition devices collaborating with terminal device.

To overcome such difficulties the transmission should be optimized depending on availability of networks, temporary throughput and delay. A quality of service and level of security based on automatic selection method shall be the basis of a flexible, reliable, secure and effective communication subsystem.

3. Main S&T Results/Foreground

1.2 User Requirements & System Design

The results of the work have been published in the following deliverables

D 1.1 Scenario list: deficiencies, handling
D 1.2 Data handling guidelines
D 1.3 Vision and requirements of the future
D 1.4 Embedded system and communication architecture

The consortium had several discussions with the border guards about the actual procedures at the borders. The stakeholders (Rumanian and Spanish Boarder Guards) expressed their needs during two workshops – one in Galati (Rumania) on 22.-23. July 2014 and another in Madrid (Spain) on 15.-16.September 2014.

During the Romanian and Spanish site survey (that took place in same time with the Galati and Madrid workshop, described above), the MobilePass Consortium members had an real scenario insight to see the live border crossing control methodology and instruments, performed on the real travellers by the real border police officers.

Live demonstrations at borders with already existing equipment had been carried out. This was a pre-requisite for a good understanding of the requirements where mobile devices are needed. Potential improvements where discussed and deficiencies of existing equipment where mentioned. Results had been summarized in D 1.1. Preliminary requirements have been captured to be formulated in D 1.3

During the site survey in the MobilePass Requirements Workshop in Galati, Rumania. Scenarios, deficiencies, handling problems and workflows for different passengers and necessary identity checks had been discussed. Exceptions are handled in a second line. D 1.1 also contains a comprehensive overview of available devices and a comparison with disadvantages/advantages of used devices. It describes handling problems and possible improvements. A novel system architecture described in D 1.4 allows the device to be used used in a distributed environment. Together with the future requirements list this vision was formulated in D 1.3. It has open interfaces, can be used standalone or in combination with other devices. A similar prototype is available now at the end of the project.

MobilePass communication architecture overview is described in D 1.4. There is a multiple path long range communication to the background information systems available and a short range data acquisition network. It allows maximum flexibility.

1.2.1 Requirements

The MobilePass requirements have been determined based on stakeholders needs. The stakeholders (Rumanian and Spanish Boarder Guards) expressed their needs during two workshops. A detailed requirements catalogue is available. In total 201 requirements had been listed. They are also the basis for the generation of the test plans in WP 3, 4 and 5.

The requirements have been expressed as a hierarchical structure where high-level requirements have been further divided into more detailed low-level requirements. High-level requirements only contain general statements and group the low-level requirements. Furthermore requirements are split into main categories and sub-categories.

Main Categories	Sub categories
Mobile Device and Software	Functionality
Communication Requirements	Usability
Application and IT Database	Reliability
	Performance
	Supportability
	Design
	Physical
	Safety

1.2.2 Future System Architecture

The requirements have been transformed into a future system architecture/design for a mobile device (combination) for passport reading, facial and fingerprint verification. Part of this system design phase was also an in depth data communication investigation leading to a secure communication design. Together with all technical partners a vision of a mobile solution was formulated and described in D 1.3 The workflow for a distributed architecture also was defined.

1.2.3 Device Vision and Architecture

The result of workshops and discussions with border guards, manufacturers and researchers formed a device vision. The device can be used in combination with existing devices and it enlarges the field of operation for border guards with face and finger scanning technologies. It is not the final form but it is a well thought-out design study. There is a 3D model available and after finishing this document the MobilePass consortium will have a 3D printout of this device as a mock-up. This was an improvement for discussions about usability and ergonomics.

Documented results in D 1.3 also lists details for a future device about the

- Camera system
- Finder display
- Illumination
- Central CPU system
- Power consumption
- Operating system and software interoperability
- Trusted Platform Module for platform integrity
- Ideal algorithm Integration
- Handling comfort
- Face capture
- Fingerprint capture
- Document scanner functions

1.3 Ethical, societal and Legal Aspects

The results of the work have been published in the following deliverables

D 1.2 Data Handling Guidelines
D 2.2 Guidelines in real life scenarios
D 2.3 Ethical, fundamental rights and societal evaluation of MobilePass
D 2.4 DPA Approval Copies
D 2.5 Implications of biometrics-bases mobile border control-final

The work has consisted of three main steps: identification of issues and risks (D2.1, D2.5), development of Guidelines (D2.2), and final evaluation and follow-up of Guidelines compliance.

Privacy and ethical aspects of data collection have been studied and for data acquisition a procedure was developed (informed consent). A major importance is given to privacy and data protection concerns within MobilePass. All the research work is compliant with the national and European confidentiality requirements.

UM--MERIT produced an overview of the types of personal data that are used in Mobile Pass and of the different R&D activities for which these personal data are processed. Applying the relevant legislation and regulations, the data handling guidelines for research and testing activities in the Research & Development work packages in MobilePass (WP 3, 4 and 5) were specified.

These include the description of a structure of responsibilities for data protection within MobilePass and detailed information on the procedures implemented for data protection, data minimisation, and data limitation in the different work packages. Also, the consortium was provided with detailed information on the procedures that will have to be followed for the recruitment of human volunteers. As an Annex to Deliverable 1.2, a sample informed consent form and an overview of the (relevant parts of) the European data protection framework was provided.

The consortium also designed a consent form for the biometric and passport data collection that the volunteers will have to fill in during the upcoming testing phases of the project.

The fact that the device reached this stage at all is a positive accomplishment, and the tests run did yield valuable information about not only the technical performance, but about the potential for socio-ethical acceptance by the users (both border guards and travelers) as well. The data currently available indicate that this potential is clearly positive.

The preparation, organization, and execution of the tests complied with legal, social and ethical requirements: much care was taken to inform volunteers adequately, acquire their free consent in written form, and collect their feedback and comments. While the preliminary results of the tests show a performance quite satisfactory for the device in its current stage of maturity, they also indicate that some aspects need further improvement and more rigorous assessment for a wider, more representative population, before wide application is justified from a LSE perspective.

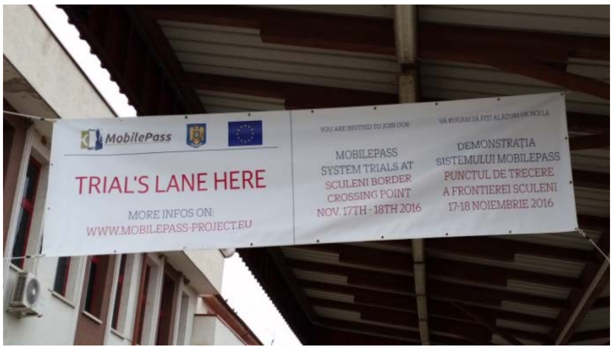


Figure 1: Banner at border and signature list for volunteers

To ensure that MobilePass complies with EU data protection rules, the Ethics Advisory Board had an eye on all topics concerning data protection. For the demonstrations we had the Approvals from the data protection agencies. To ensure that data captured is safe, we defined the Data Controller and Data Processor and Sub-Processor roles and signed defined agreements.

Volunteers signed the informed consent paper, available in different languages (Romanian, Russian and English). The demonstration was clearly announced with flyers, on the Web and with banners on the border one week before actual test. Feedback was taken from travellers and border guards after procedures and tests. Guidelines in real life scenarios had been followed as much as possible. E.g.: MobilePass Members had to wear specially designed jackets.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

Figure 2: volunteers list and signatures for free consent

A set of guidelines has been sent to the border guards to assess the situation as a whole. In combination with AIT ideas to set up the demonstrations (objectives, involved travellers, involved persons, real data, simulations, etc.) the border guards came up with a rough idea and answers to the guidelines. In a process of several telephone discussions, we clarified questions and situations and had finally answers to fulfil the guidelines.

These answers were the basis of the demonstration design. How they had been followed is depicted in the Demonstration Report D 7.1

The consortium endeavoured to follow the following guidelines:

- Planning and Preparing the demonstration
- The demonstration plan SHOULD comply with existing standards for testing of biometric systems
- The relevant Data Protection Authorities MUST be notified before demonstration takes place
- Involvement of travellers and border guards as test persons
- Border guards SHOULD NOT experience disproportional benefits/costs due to their participation in the demonstration
- Travellers SHOULD NOT experience disproportional benefits/costs due to their participation in the demonstration
- Selection of test subjects
- The test subject population that is recruited SHOULD be as representative of the target population as possible
- It may be necessary to selectively recruit volunteers in order that the test subject population is as representative as possible, and does not underrepresent known problem cases

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

- Travellers SHALL only participate as test subjects in the demonstration on the basis of free, explicit, and informed consent.
- Test subjects MUST be provided with information about data processing in the context of the demonstration and about their rights
- The data controller SHALL establish procedures for withdrawing consent and for exercising test subject's rights (right to erasure, rectification)
- Set-up of Demonstration
- The personal data of test subjects (travelers) SHALL BE processed strictly for the purpose of evaluation of the MobilePass device (and not for border control purposes).
- The demonstration site MUST be spatially and organizationally separate from the actual border processes.
- When personal data of test subjects (travellers) are processed during the demonstration, compliance with data protection regulations MUST be ensured
- When evaluating the system in terms of its potential to 'increase the speed and security of border crossing' (see principle of proportionality), an explicit methodology SHOULD be developed.

1.4 Mobile Computing Platform & Passport Reader

The results of the work have been published in the following deliverables

D 3.1 Device Specification
D 3.2 Test plan preliminary version of prototype
D 3.3 Traveller Authentication Device
D 3.4 Integration Report and Device Evaluation (Pending at the time of writing the report)

1.4.1 Passport Reader:

Regula delivered 6 samples of the prototype to: AIT, Veridos, Spanish Border Guard, INDRA (2x), Romanian Border Guard. This was necessary to integrate the prototype into the workflow system. Veridos used the SDK provided by Regula and implemented an interface which also works via wireless communication channels. AIT and Veridos optimised the sized and data formats for a much faster communication between devices. There is also a novel version of the passport reader available, but unfortunately it was not able to get it integrated at the demonstration. Preliminary tests showed that the RFID reading is up to 40% faster on

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

the new device, speeding up the time to read RFID data (passive, active authentication, face and fingerprint information) from 17 seconds to approximately 10 seconds.

To test the functionality in the labs we used fake "UTOPIA" passports, manufactured by Veridos. AIT had 10 volunteers (informed consent documented, data protection guidelines apply) who provided their faces and 2 fingerprints (index fingers) for production of these passports. For these passports we have the certificates to also read the fingerprints via EAC (extended access control). This enabled us (for preliminary tests and factory tests) to close the complete chain from eMRTD reading until fingerprint verification on the device. The used passports had the same chip access interfaces and security protocols like real passports. Optical security features are available but features are not in the known documents database from Regula as these passports are from UTOPIA. During preliminary tests some improvements in the interfacing were done, also some bugs had been corrected for proper operation. Regula helped in configuration of the passport scanner, working closely with INDRA and VERIDOS. For preliminary checks, Regula provided a possibility to store local certificates in the reader itself, so Veridos and INDRA were able to perform local tests also.

1.4.2 Computing Platform (MobilePass Device)

The task in the second period of the project was to integrate the elements, hardware components and software libraries (facial verification, fingerprint verification) and provide interfaces for integration in WP 6.

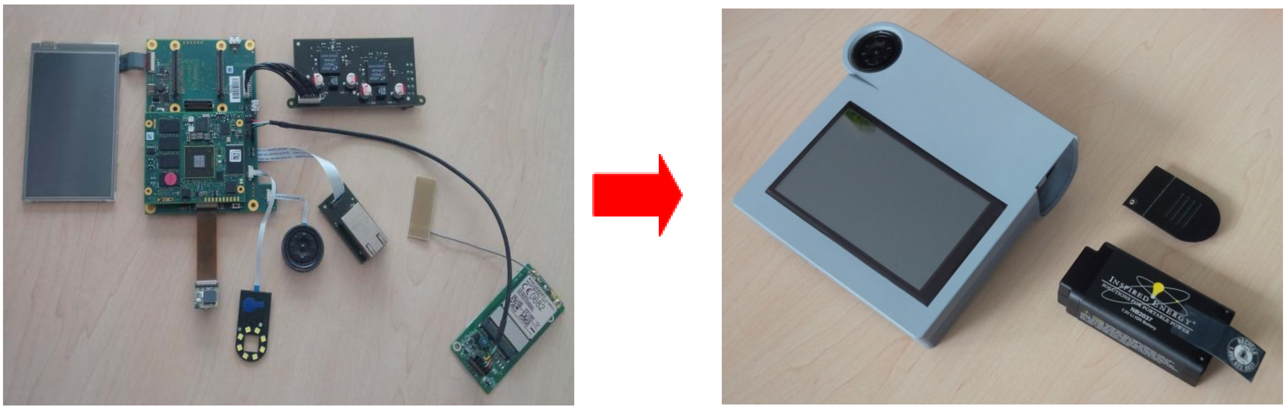
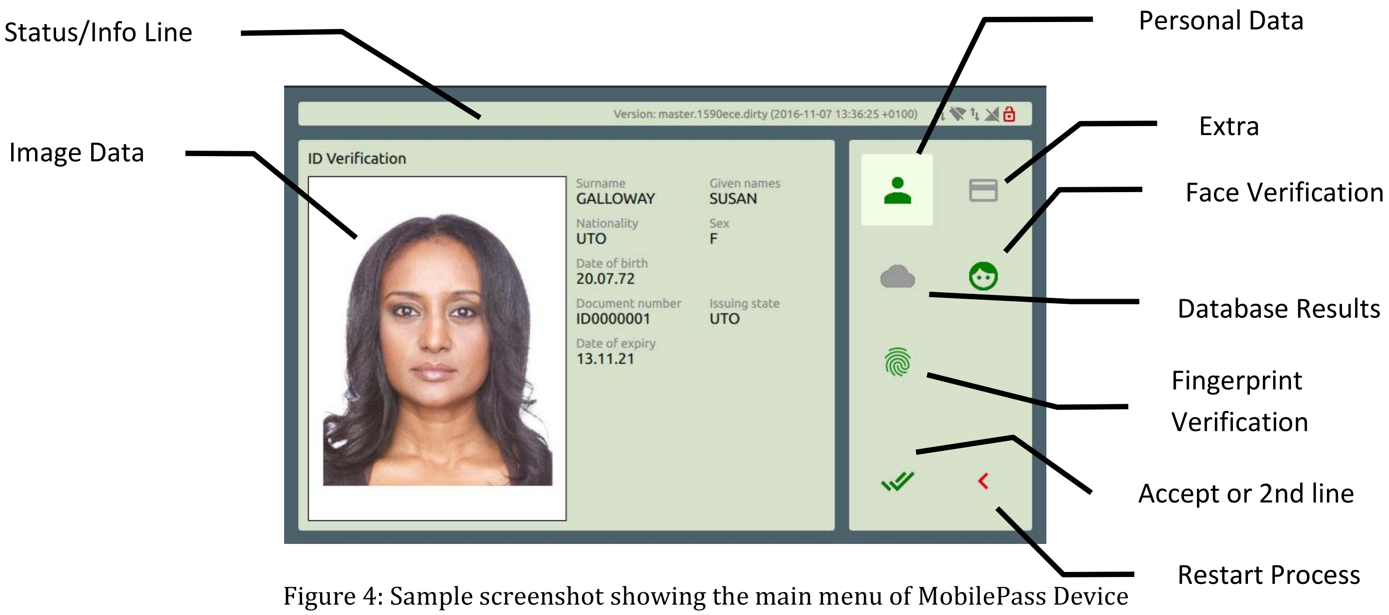


Figure 3: Hardware elements for integration in biometric check device

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

Fraunhofer, together with AIT, did a user interface to show functionalities in a simplified form. AIT provided the development toolchain for embedded development. More screenshots and a complete user interface description can be found in deliverable D 6.4 Subsystems Integration report and system manual.



Version: master.1590ece.dirty (2016-11-07 13:36:25 +0100)

ID Verification

Surname
GALLOWAY

Given names
SUSAN

Nationality
UTO

Sex
F

Date of birth
20.07.72

Document number
ID0000001

Issuing state
UTO

Date of expiry
13.11.21

Figure 4: Sample screenshot showing the main menu of MobilePass Device

Figure 5: Final MobilePass Device, fingerprint scan procedure

1.5 Fingerprint Acquisition and Biometric Recognition

The results of the work were published in the following deliverables.

D 4.1 Test plan and preliminary version of device
D 4.2 Fingerprint capture module
D 4.3 Algorithm Library for Fingerprint Image Enhancement
D 4.4 Algorithm Library for Fingerprint Verification and Interoperable Feature Extraction
D 4.5 Evaluation Report

Fingerprint is one of the oldest biometric modalities and the first one to be studied through a scientific method. WP4 work was centred in developing contactless fingerprint technology to be used for border control in open scenarios.

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

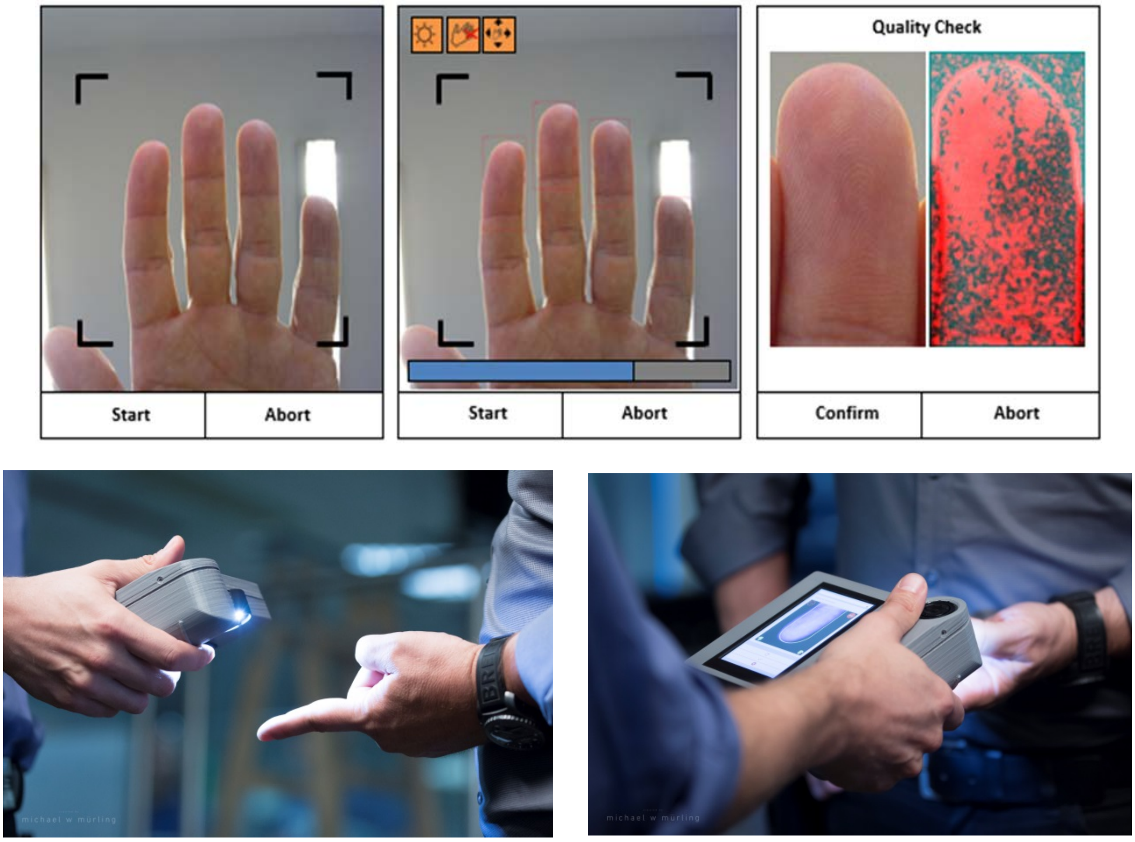


Figure 6: From design to real implementation

Starting with the strategy outlined in the project proposal, WP4 has worked in close contact with our end-users. These talks with end-users have made to change the strategy, as new requirements dealing with interoperability have to be considered. With these new requirements, a new solution has been proposed and an important focus was demanded for an *a priori* checking of the quality of the images before entering the comparison process. The fingerprint recognition and matching was completely implemented an integrated into the device. It is now possible to verify a digital image of a fingerprint with an image taken by the MobilePass camera. The algorithm only takes images of sufficient quality for matching purposes. A user interface shows the live matching score and an indicator gives "green" light when matching is above threshold. ~1600 fingerprints had been captured anonymously and used for evaluation purposes. At the time of writing this report the fingerprints had been destroyed. The first implementation of the fingerprint matching algorithm was with the free available NIST library. We have known that there are commercial implementations around which are better. We visited the company Innovatrics in Bratislava and they had been willing to port the algorithm to our hardware. At the moment the device can be operated with two different fingerprint matching algorithms.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

In the initial plan of the project, the idea was to develop a new fingerprint recognition algorithm, but following conversations with end-users, it was found that the strategy should follow the adaptation of existing algorithms as to provide both, interoperability and universality. One of the possible variations of a real scenario is the requirement by the end-user of not performing the fingerprint recognition inside the terminal, but in a remote server. Reasons for this may vary, but may go from security and privacy concerns, to the confidence in the recognition tool they have independently acquired from a third party. Also depending on external parameters, such as the current alarm level, the end-user may like to raise the comparison threshold, as to allow more accurate recognition, even though an increase in the rejection rate is obtained. But one fix characteristic in all real scenarios is that the images captured with the MobilePass device will never be compared with other MobilePass images, but with images taken with traditional optical sensors. These images will be read from the passport and internal databases.

The above mentioned situation states a set of requirements that have modified the initial specifications during the execution of MobilePass project. These requirements are:

- The fingerprint recognition algorithm shall be able to manage minutiae.
- If the algorithm is to be executed inside the MobilePass device, its computational cost shall be low.
- The fingerprint recognition algorithm shall allow the comparison of MobilePass images with traditional optical sensors, i.e. interoperability among capture devices has to be achieved.
- The images acquired by the MobilePass device shall be able to be used by different fingerprint recognition algorithms, i.e. interoperability among biometric recognition algorithms shall be guaranteed.
- In any case, the MobilePass device shall ensure that the image acquired is of enough quality and containing enough information to ease the capturing process and lowering the error rates.

Therefore, the work in WP4 has focussed the following terms:

- A low-computational cost minutiae-based algorithm will be developed. The point of reference has been the open-source NBIS algorithm supplied free of charges by NIST.
- Images acquired by the MobilePass device will be converted to 8-bit gray scale, as to be compliant with other algorithms.
- In addition to the pre-processing techniques detailed above, further image enhancement and quality checking will be added as to adapt the image to reach an equivalent quality than the one of a life scanner.

- Images will be coded using ISO/IEC 19794-4 and quality checking will be compliant with ISO/IEC 29794-4.

With these final requirements, a minutiae-based algorithm has been finalized and preliminary evaluated. The evaluation performed is composed of two different evaluations. The first evaluation is a scenario evaluation that is based in emulating the conditions in a border control and using the fingerprint module from the MobilePass device. The second evaluation has been an evaluation under operational conditions, where feedback about the user of the system, plus the analysis of the fingerprint images captured has been obtained. The evaluation is composed of several tests, which include the technological evaluation of the quality assessment, analysis on the acquisition time for a sample within an attempt, performance evaluation both within the MobilePass device and simulating a real scenario, and a usability evaluation. In addition, this scenario evaluation encloses different tests:

- Quality evaluation: 3 different algorithms for quality assessments
- Time Evaluation: 7 different acceptance criteria for each attempt
- Performance Evaluation:
    - MPD vs. MPD performance
    - Real Scenario, by enrolling with RSD and verifying with MPD

The results show that NFIQ1 presents a very low discrimination capability and there are also erroneously scored samples, while NFIQ2 and a commercial algorithm present a similar behaviour, being a bit more discriminative NFIQ2 due the easiness in saturating the commercial alternative. But using the commercial product for the quality threshold may be a better option for those cases where FNMR has to be forced to a very low value.

When using both comparison algorithms, the one developed within WP4 and a commercial one, it has been proven a high level of interoperability between the images captured and processed by the MobilePass device, and both algorithms. The performance obtained by the commercial algorithm is better, but it also shows that any other commercial algorithm could be used.

In a nutshell, the results obtained are:

- From the quality assessment part:
    - The use of NFIQ1 is not recommended due to its lack of discriminative power, as well as its weird behaviour with many images.
    - Although still in its beta version, NFIQ2 shows a reasonable behaviour and a not so high computational power.
    - The 1st version of the commercial algorithm behaves as NFIQ2, but with a bit more computational demand.
    - The 2nd version of the commercial algorithm loses the discriminative power and consumes more computational resources.
- From the interoperability point of view:

  - It is guaranteed that the MPD images can be processed by different algorithms.
  - The performance of the recognition algorithm included in the MPD achieves a medium performance, while the commercial product improves such performance.
- From the usability point of view:
  - The time required to acquire a sample that overcomes the acceptance criteria could be lowered to improve operator acceptance.
  - The effectiveness achieved by the fingerprint device has turned out to be excellent, as only 1 single case of not acquisition has been found in the operational evaluation.
  - Both travellers and operators have shown great acceptance to the new technology.

1.6 Cooperative Face verification development

The results of the work have been published in the following deliverables.

D5.1	Report on evaluation dataset
D5.2	Test plan and first preliminary version of device
D5.3	Algorithm library for face image enhancement
D5.4	Algorithm library for face tracking verification
D5.5	Evaluation report

The objectives of WP 5 were to investigate, to implement and to evaluate algorithms for cooperative face verification, including face detection, best-shot selection and image enhancement as necessary building blocks for implementing face recognition on a mobile device.

After the collection of domain-specific test- and training data and the construction of a preliminary device in the previous reporting period, the ground has been laid for the development and evaluation of dedicated mobile face-recognition algorithms in this reporting period.

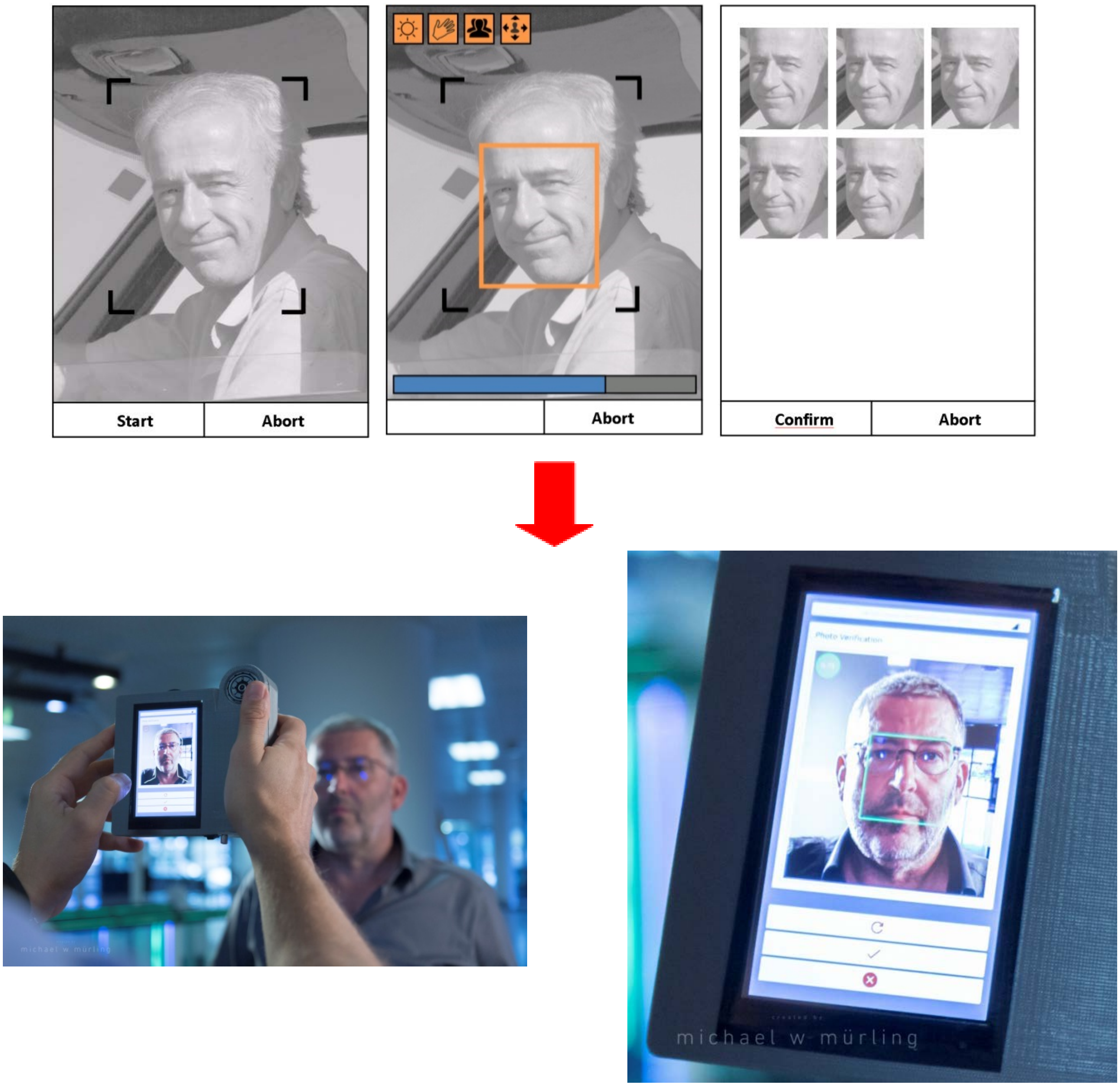


Figure 7: From design to real implementation

New algorithms were implemented for facial landmark localization and template extraction. Compared to the pre-project baseline, the speed of the algorithms was improved by a factor of 20 for landmark localization and a factor of 5 for template extraction. Likewise, the memory consumption was reduced by a factor of 7. Furthermore, a real-time asynchronous face-processing chain was implemented to utilize multiple CPU cores. The facial recognition and matching was completely implemented an integrated into the device. It is now possible to verify a digital image with an image taken by the MobilePass camera. The algorithm only takes images of sufficient quality for matching purposes. A user interface shows the live matching score and an indicator gives “green” light when matching was positive.

Demonstration on 150 travellers in real environment was done. Evaluation on much more images in the lab was done.

An evaluation of the algorithms showed that the face-recognition performance on community datasets is excellent under conditions comparable to the MobilePass scenario (e.g. Feret, FRGC, to some degree also FOCS “good”) and still adequate under more adverse conditions (FOCS “bad” & “ugly”, MBGC, LFW, YTF). When comparing the results to other systems it should be noted that this is a very fast algorithm for video-rate face recognition on hand-held device with a very low resource footprint.

For landmark localization, this was done by implementing a new algorithm to replace the SIFT-like features from the baseline system by fast pixel-based features, followed by a new efficient tree-based classifier. The new algorithm was trained with ~10,000 labeled face images and evaluated to make sure that it matches the quality of the original algorithm. As a result, the speed of landmark localization could drastically be improved from formerly 474ms to now 23ms per face on the MobilePass mobile platform.

Being the most crucial and also computationally expensive step of the processing chain, a large effort was spent to speed-up the template-extraction algorithm. Compared to the baseline algorithm, the processing time for one face reduced from 1094ms to 196ms. In both algorithms, a similar kind of local features are used, but the new algorithm applies a hierarchy of rigorous dimensionality-reduction steps that aim to keep the feature-vector size low - and thereby the CPU usage, too. The in-memory size for the internal transformation matrices the algorithm relies on was reduced from 143MB to now 20MB. Likewise, the size of a single face template was reduced from 8,004 bytes to a mere 888 bytes.

	Baseline	**MobilePass**
Data model size (all components)	181.5 MB	92.5 MB
Runtime landmark localizer	474 ms	23 ms
Runtime face-template extractor	1094 ms	196 ms
Template size	8004 bytes	888 bytes
Matching time (1 : 1000 templates)	9.1 ms	2.2 ms

Figure 8: Improvements in speed and memory consumption

The final face-recognition library has been made available to the integration work package for deployment in the demonstration device.

Six different publically available datasets were selected for evaluation: FERET, FRGC, MBGC, FOCS, LFW and Youtube-Faces. They are well-known amongst the face-recognition community and each of them exhibits some aspects that are relevant to the MobilePass scenario of image/video-based face recognition. Both the baseline face-recognition algorithm

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

and the final MobilePass algorithm were evaluated, and the detailed evaluation results were published in deliverable D 5.5. See below as an example the results on the FRGC dataset.

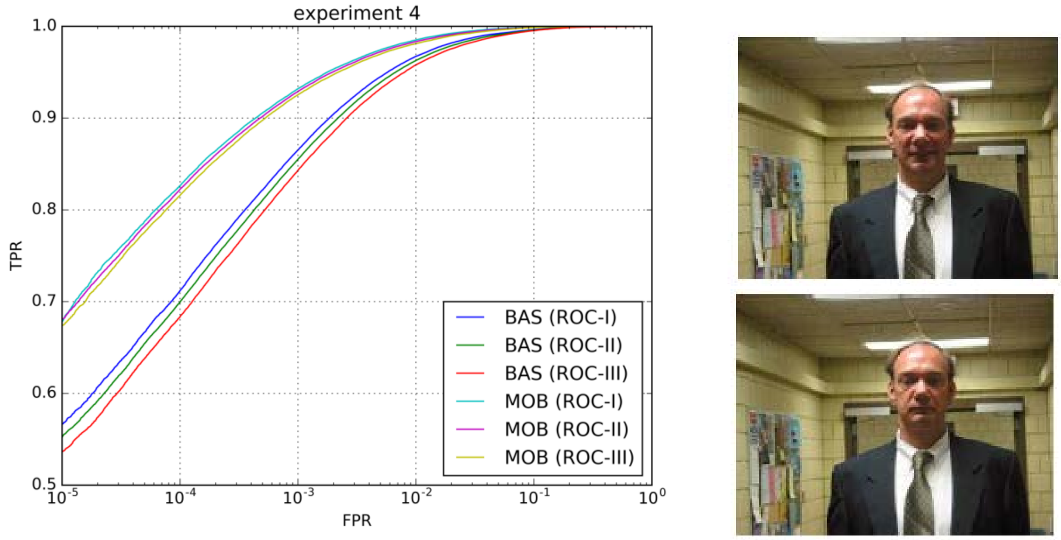


Figure 9: ROC-curve and images from the uncontrolled scenario (experiment 4) of the FRGC database. Baseline system (BAS) vs. MobilePass system (MOB) on three different subsets of the data (ROC I-III).

When comparing the results to other state-of-the-art face-recognition algorithms, please note that we evaluated the very same generic pre-trained algorithm on all datasets, i.e. the algorithm was not tweaked to the specifics of the respective evaluation dataset. While adaptation is certainly effective to produce high evaluation results, it is rather pointless when trying to assess the algorithm’s actual performance “in the wild”. See the following examples for the significant improvements that can be achieved by adapting the algorithm to the evaluation dataset.

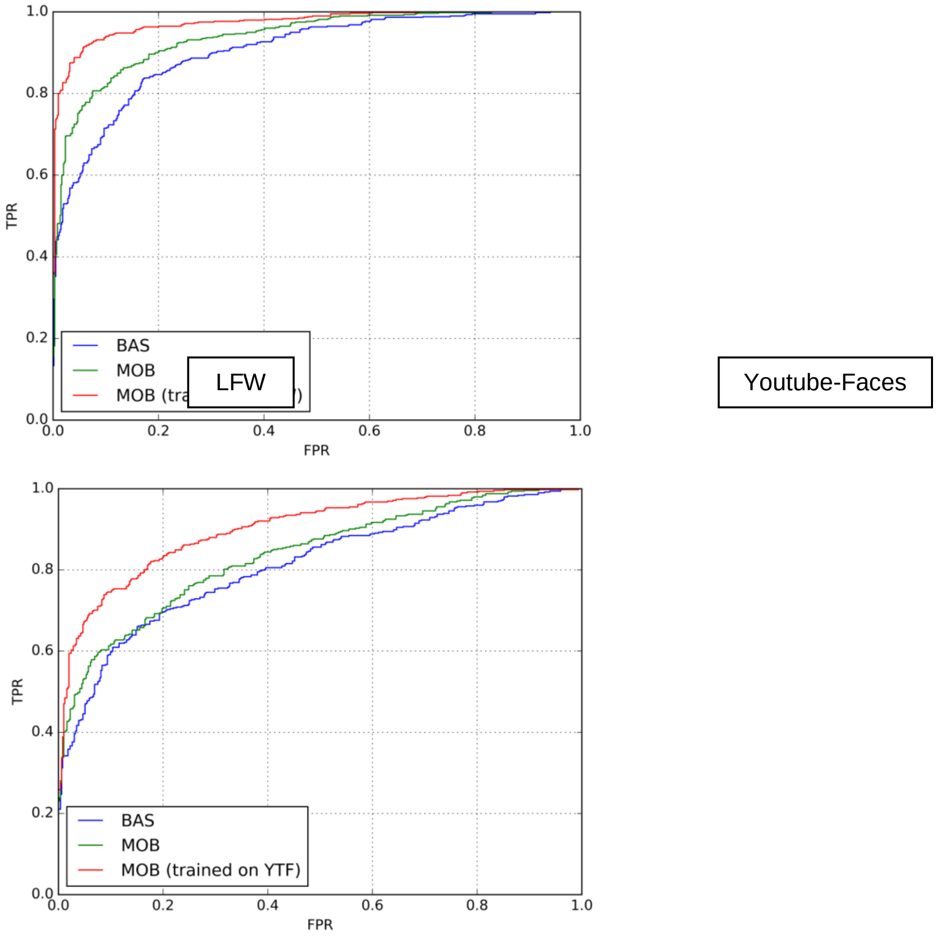


Figure 10: ROC curves for LFW and Youtube-Faces. Baseline algorithm (BAS), MobilePass algorithm generic (MOB green), and trained to dataset in an n-fold leave-one-out procedure (MOB red).

A dedicated scenario-specific dataset called “MobilePass Faces” (MPF) was recorded in the previous reporting period. It was now used as another source for evaluating the face-recognition quality and also the performance of the best-shot selection.

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

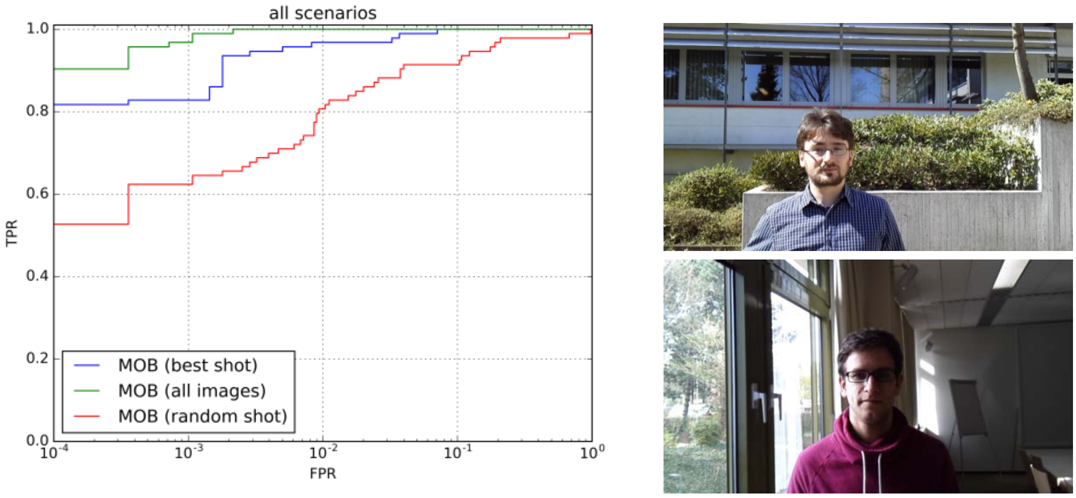


Figure 11: ROC curves for the MobilePass dataset. Best-shot selection outperformed random-shot selection clearly, but could not quite reach the theoretical optimum of using all images.

1.7 System Integration, Evaluation

The results of the work have been published/documented in the following deliverables

D 6.1 Test Results for preliminary system
D 6.2 Integrated Devices
D 6.3 Network Integration report security evaluation report
D 6.4 Subsystems Integration report and system manual

The objectives of this work package were to

i) ensure through iterative integration that all software and hardware components can work together as a system, taking into account the chosen system specification and operational requirements,

ii) assess the quality and efficiency of individual system modules developed during the project. In the final phase of the project the developed approaches as well as the overall system architecture/concept will be evaluated along the line with the defined trial specifications

The main work in this work package was the software adaption between involved elements among partners AIT, Veridos, Regula and INDRA (respectively span. Police responsible for database systems access)

The preliminary elements from the work packages WP 3, 4 and 5 have been integrated: the electronics, the device, the optical fingerprint reader. In total, 7 prototypes were manufactured.

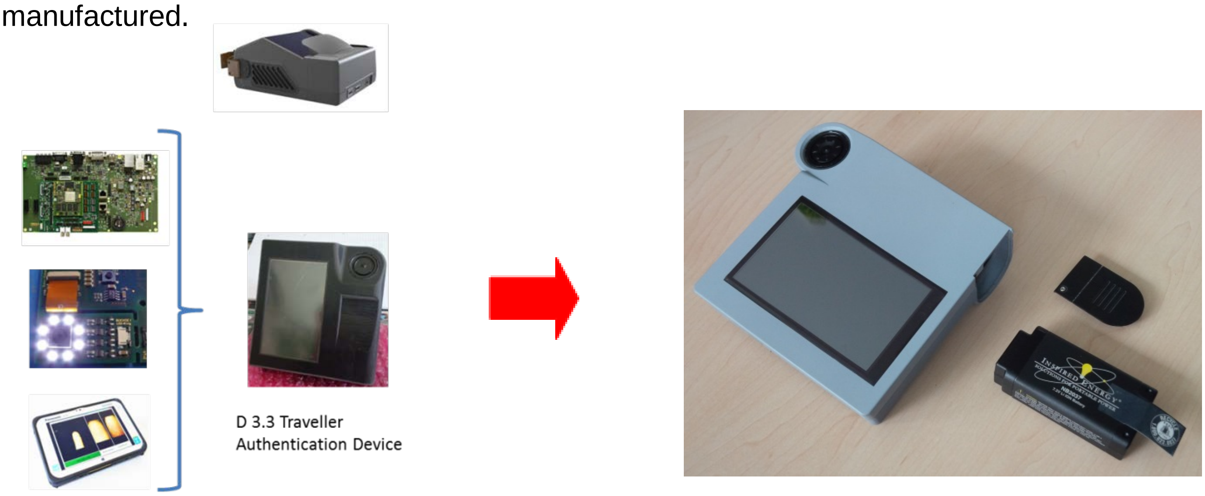


Figure 12: Various preliminary parts & elements integrated into “final device” for field operation

Furthermore, the remaining tasks for integration into a complete system had been done: integration of Mobile Device and Passport scanner into Veridos workflow system, Integration of communication protocols and the integration of the “back-end” systems (ARGOS information system for Schengen, VISA, Interpol Database access) and the connections to the Terminal Control Center (for handling of the passport certificates for authenticity and extended access control (EAC) for fingerprint access).

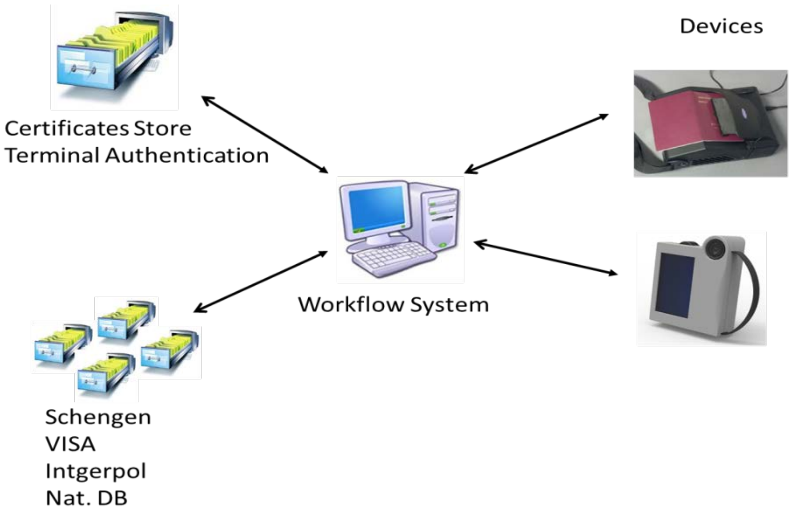


Figure 13: Database access, Certificates storage, workflow system, and mobile Devices integrated into one system

1.7.1 Step A) Integration of components

Integration of passport scanner and MobilePass Device with the Veridos workflow system. As an additional help Veridos developed 2 Mock-up's (one for the Passport reader and one for the MobilePass Device to evaluate the workflow system and simulated data in absence of the real hardware. Interfaces had been the same, so at the moment of availability only the configuration had to be changed. This version can be used as a standalone variant, without online access.

1.7.2 Step B) Integration with database systems

Integration of part a) with the database systems for "Hit-list display of the span. police, and the inclusion of the certificates store for passports. This was the task of INDRA and with help of AIT. This version only works in the context of the Spanish police environment at El Escorial (pre-production environment).

Step A

The developed WSDL communication schema for communication between MobilePass Device and workflow was fully implemented and extended in several iterations. A complete cycle of:

passport scanning, MRZ verification, verifying optical security
chip reading, verifying chip security (certificates locally stored)
crosschecks (e.g. validity) of the workflow system
facial verification and
fingerprint verification
DB access and results display (Hit-lists simulated)

can be done. For factory tests 10 UTOPIA passports have been used with local stored certificates. The following sample workflow shows a diagram Figure 13 about the communication and the exchanged messages between the systems. As an example: this workflow was used during the tests in Sculeni/Romania.

Step B

Two additional Interfaces had to be developed, to get access to certificates databases and police information systems:

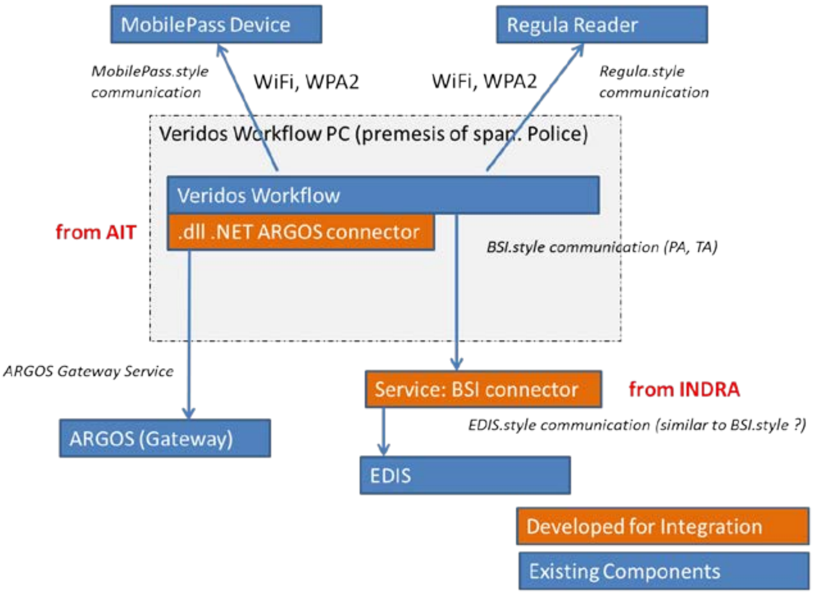

MobilePass Device
Regula Reader
MobilePass.style communication
WiFi, WPA2
WiFi, WPA2
Regula.style communication
Veridos Workflow PC (premesis of span. Police)
Veridos Workflow
from AIT
.dll .NET ARGOS connector
BSI.style communication (PA, TA)
ARGOS Gateway Service
Service: BSI connector
from INDRA
EDIS.style communication (similar to BSI.style ?)
ARGOS (Gateway)
EDIS
Developed for Integration
Existing Components

Figure 14: Interfaces view between (Version b), between Workflow system, Passport Scanner, MobilePass Device ARGOS system and certificates store for online operation

The ARGOS connector is a .DLL attached to the Veridos workflow communicating to the Spanish Police information system. This system includes several databases, as SIS-II, Interpol, National DB and VISA. The BSI connector is a service responsible for certificates exchange (in fact it consists of two separated services). This interface allows for certificates exchange between the passport reader and the terminal control centre (EDIS).

The developed communication between the passport reader the workflow was fully implemented and extended in several iterations. In addition to functionalities in step A, the following functions are implemented:

- Implementation of a VPN network in order to get access to government services.
- Implementation of the ARGOS Interface to get access to the SIS-II, VISA, Interpol and national Databases.
- Passive Authentication (PA)
- Terminal Authentication (TA)

Preliminary and final test plan results are available. See sample extraction of test plan results in next table of Deliverable 7.1, Demonstration Report.

BDF-001-8	The Device must read the data from the EF.SOD data group the Document Security Object	OK
BDF-001-9	The Device must read the data from the EF.COM data group the Common Directory File	OK

BDF-001-10	The device must do a EF.SOD verification and a comparison between EF.SOD and EF.COM.	OK
BDF-001-11	The device must do a DS certificate signature verification, a Certificate validity period check and check the DS certificate revocation status. *Comment: the device does a DS certificate signature verification. There are three methods available:* Update device manually, store local certificates: this is actually implemented. Actually required certificates can be transferred to the device using online methods without saving them to the device. Regular updates of the revocation list and certificates on the device without updating whole software for example sync with the network share *It is recommended to split this requirement into two separate ones.*	partly
BDD-015-1	The system must check the falsification attributes of the document (visible light, UV, IR)	OK
BDD-017-1	The system must check the falsification attributes of a document under UV light (UV dull paper test). *Comment: The passport reader device does a UV dull paper check, but results are not transferred to the MobileDevice, integration pending.* *It is recommended to split this requirement into two separate ones.*	partly

Figure 15: Example excerpt of test plan results of demonstration in El Escorial/Spain

1.8 Demonstration

A three-day demonstration took place in Sculeni/Romania at the border between Romania and Moldavia and there is an ongoing technical in-depth demonstration at the Spanish pre-production environment of the police in El Escorial/Spain.

Figure 16: Demonstration & Evaluation team at Sculeni Boder (wearing EU/MobilePass designed jackets) and Border Police from Romania

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

In total, about 150 travellers have been checked with the novel devices, feedback from the travellers as well as from the border guards was very positive.

A three day demonstration took place in Sculeni/Romania at the border between Romania and Moldavia and there is an ongoing technical in-depth demonstration at the Spanish pre-production environment of the police in El Escorial/Spain.

The overall purpose of the demonstration in El Escorial/Spain is on connectivity to the Background systems and certificates exchange. In contrast to the Romanian demonstration a small number of simulated travellers are tested to have more time to concentrate on the integration and data flow issues.

The MobilePass device was tested in various situations (car, busses, indoor, outdoor, different light situations, different travellers and different operators). The situation was a simulated one, no Schengen System or VISA access was done, but it was simulated: e.g. when the traveller was entered in the simulation database, a hit was displayed on the device.

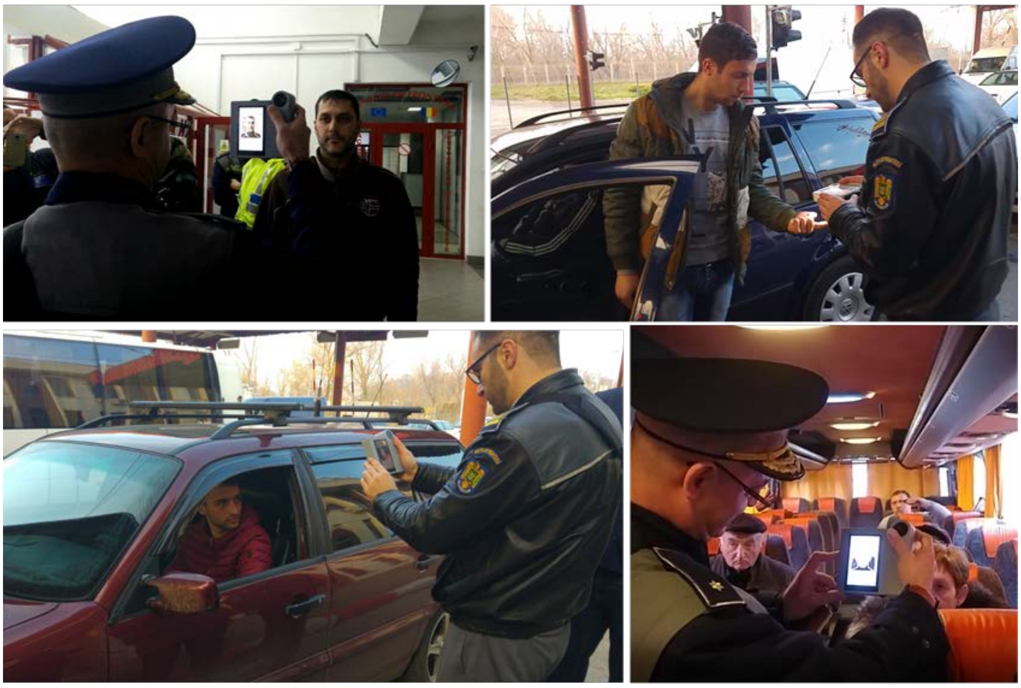


Figure 17. Scenarios during the MPD (MobilePass Device) evaluation

To ensure compliance with EU data protection rules the following setup was chosen. The evaluation workflow is depicted in Figure 17. The first step (and mandatory) for all travellers is to complete the current border check (RBC -Romanian Border Check- in). Then, those travellers who voluntarily decide to participate in the evaluation proceed to step A, where an

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

operator explains the whole process. Signing an acceptance sheet is mandatory to participate in the evaluation. Once the consent is signed, the traveller starts the step B where the passport checking and the face recognition are carried out by an operator. Then, the traveller proceeds to step C, where other operator captures her fingerprints (both index). Finally, the traveller is requested to complete a survey in step D and finishes the evaluation. The MPT is present during the whole process to overcome any possible inconvenience.

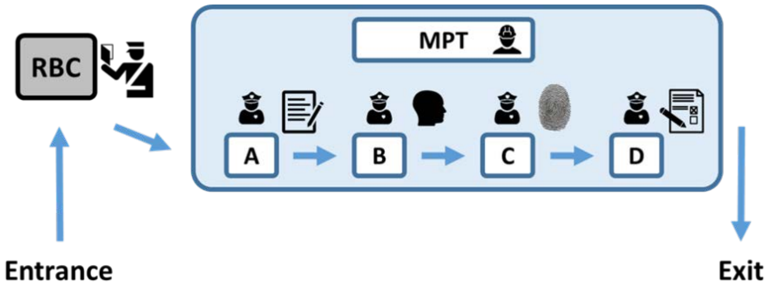


Figure 18. Mobile Pass evaluation workflow

	Day 1	Day 2	TOTAL
AVG	36,74	38,05	37,52
STD	16,93	21,05	19,40
MAX	85	118	118
MIN	17	20	17

Table 1. Average time (AVG), standard deviation (STD), maximum (MAX) and minimum (MIN) time of the travellers' interaction during day 1, day 2 and in total (in seconds).

1.8.1 Feedback Travellers

- 90% find the MobilePass Device easy, fast and comfortable.
- 90% find biometric recognition simple and convenient.
- 95% of the travellers think the MobilePass Device is an improvement of the current system.
- Only 2,2% of the travellers do not trust in the MobilePass Device security.
- 22% of the travellers would not trust in a smart-phone based solution.
- Improvements suggested by travellers include: increase the procedure speed (and therefore, decrease the time) and introduce more user-information at the beginning.

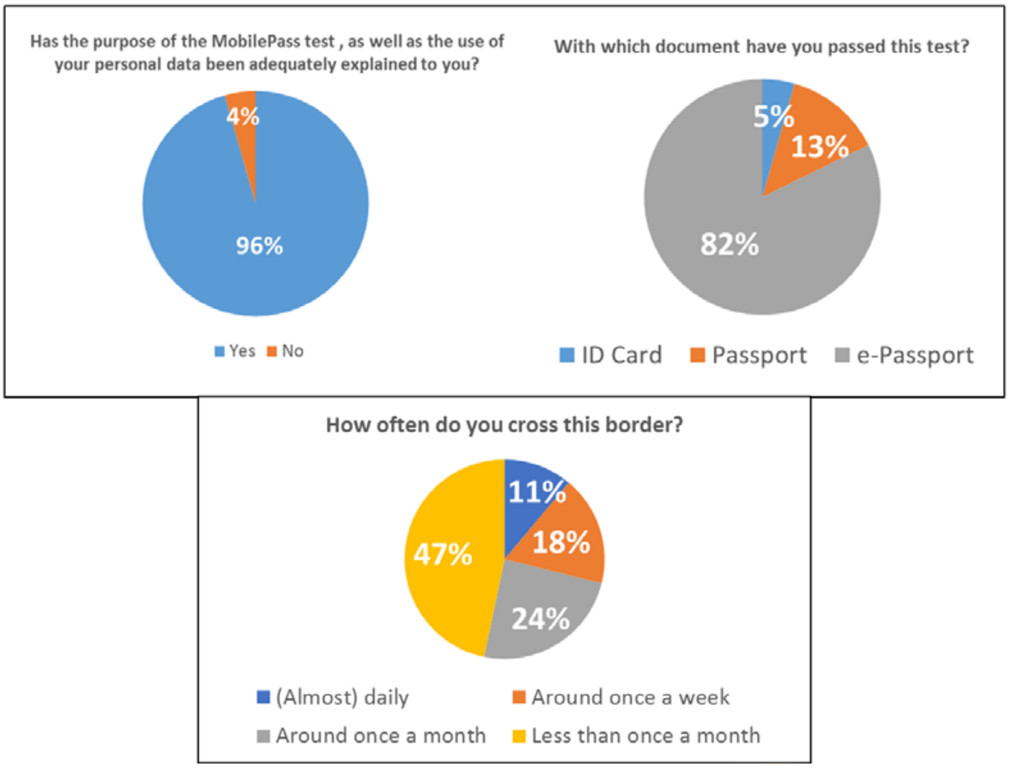


Figure 19. Questions regarding the experiment, documentation and frequency of border crossing.

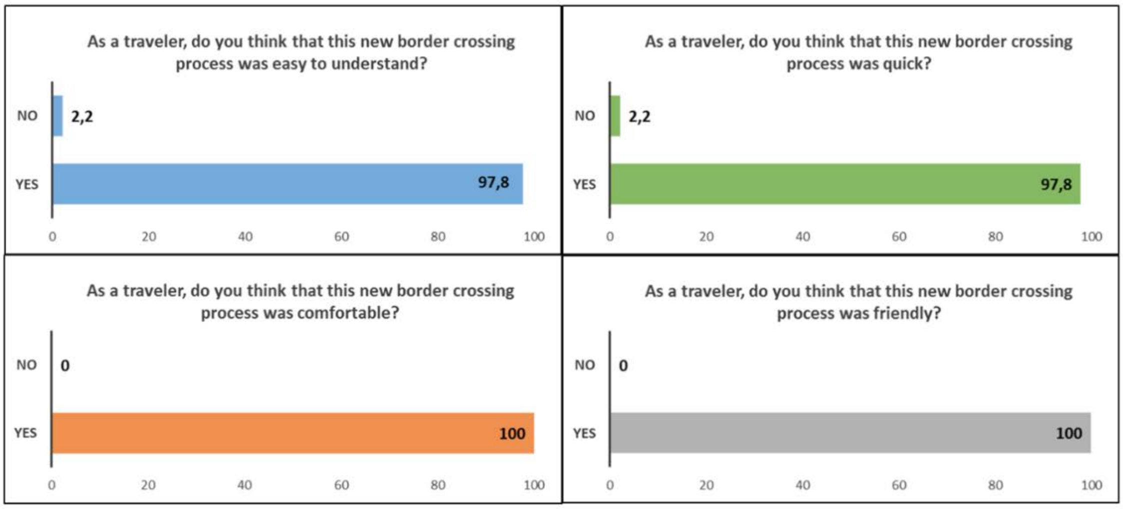


Figure 20. Questions regarding the easiness, speed and comfort of the new border crossing.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

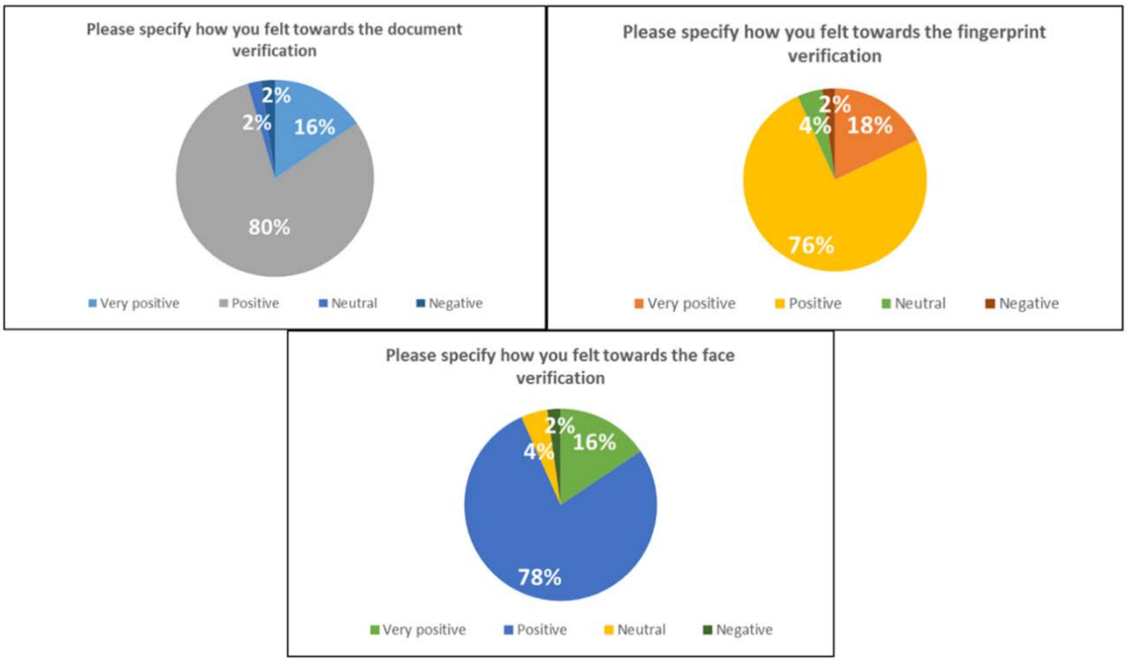


Figure 21. Questions regarding travellers' experience during the different experiment phases.

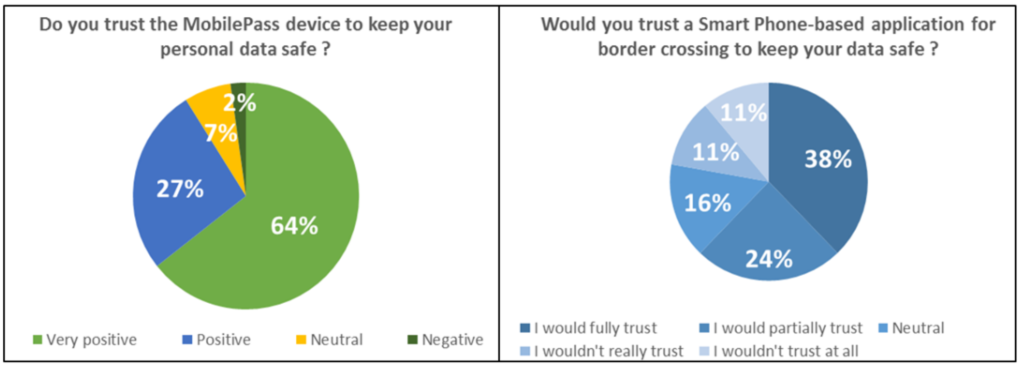


Figure 22. Questions regarding data security within the MPD and other mobile devices.

1.8.2 Feedback Romanian Border Guards

- 5 Romanian Border Police cited the lightning as an influential factor and noticed lightning differences between mornings and afternoons
- Travelers feel confidence after the first explanation.
- Only a little percentage of travellers felt reticent about fingerprint recognition.
- Most of the Romanian Border Police would use the Device daily.

This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

In the following figures, the surveys' answers of the RBP are shown. Each number of the figures' Y axis represents a different person. A total of 7 Romanian border guards who participated in the experiment completed this survey.

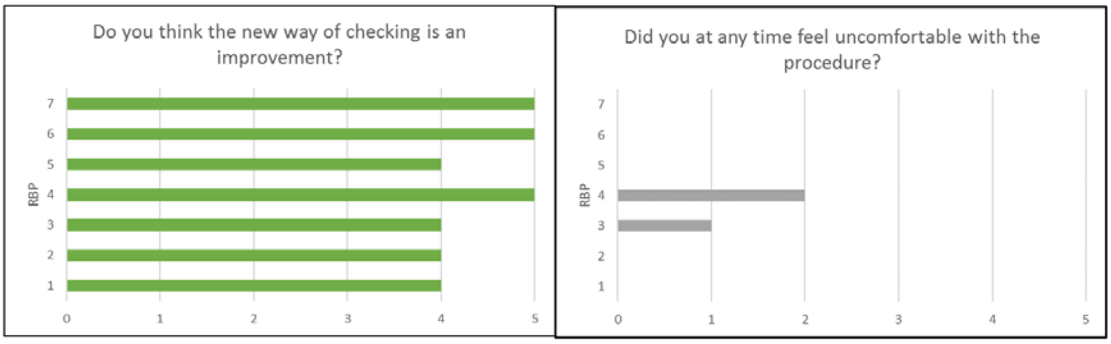


Figure 23. General questions about the MP procedure. X axis is a mark from 0 (not at all) to 5 (yes, a lot).

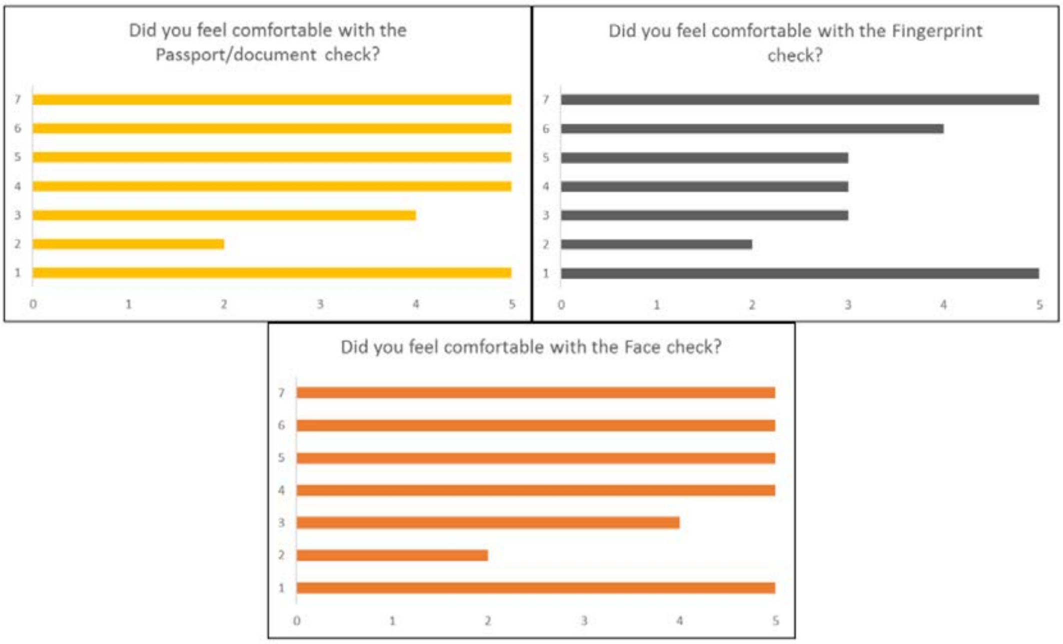


Figure 24. Questions regarding comfort with the different phases (document, fingerprint and face recognition). X axis is a mark from 0 (not at all) to 5 (yes, a lot).

4. Impact

MobilePass research and development focused on next generation mobile equipment for biometric passports. Hereby, the project outcomes follow three main categories of impact:

- Impact on future mobile systems in European border control (socio-economic impact, wider societal impact)
- Dissemination: novel technologies for mobile passenger check
- Exploitation of research results

1.9 Socio-economic impact and the wider societal implications

1.9.1 Impact on mobile border control from a member country perspective

The MobilePass project aimed to address issues relating to the optimization of the border control process at both the practical and security level. The practical experience and guidance emerged from the project work are of relevance to an array of stakeholders within EC and beyond, and will be of value across different sectors and internationally. Results of demonstrations and developments had been distributed to several border guards in different countries and disseminated also in various workshops (e.g. FRONTEX). A lot of valuable information was given to the members states LEAs.

Results of the demonstrations in Romania and Spain gave practical hints to the decision makers, purchasers and implementers of novel mobile biometric devices. Results and Feedback from border guards had been very positive and they are looking foreward for further collaborations.

MobilePass was invited to be part of Frontex Field Operations. The Coordinator and a Member of the Project Advisory Board visited the operational area of Frontex Joint Operations - Flexible Operational Activities – Röszke Border Crossing Point and Border Surveillance Area at the Hungarian-Serbian external land border. During this visit a (offline) MobilePass demonstration was done. Hungarian Border guards commented very positively about the new developments.

1.9.2 Security industry

Novel technologies had been implemented, tested and evaluated with in MobilePass. The relevant technologies had been developed within Europe by several SME´s. This gives EU industry technological advantages and additional knowledge for future developments.

The fact that contactless fingerprint scanning was shown and demonstrated for the first time at a real border gives an industry push and showed the huge potential of this novel technology. Besides this, also payment industry and payment service providers have put an eye on contactless fingerprint scanning. It is likely of using contactless captured fingerprints as a second factor for authentication.

Regula showed a full-page passport scanning technology in real field, full integrated in a wireless solution. Veridos showed the interconnection and the solution of a dedicated workflow system with two different devices via radio transmission. All MobilePass partners are active in an international market. INDRA did software adaptions and developments for passport certificate exchange and background information systems adapters. Videmo enhanced their face recognition and matching software and ITTI did advances in network communication switching technology all on embedded devices.

In addition other SME´s had been addresses during and after MobilePass developments: e.g. electronic & industrial design companies, providers of biometrics matching algorithms and embedded software houses.

1.9.3 Future Research

Research institutions like AIT, Fraunhofer and Universities like UC3M and UNU-MERIT have shown that they are inline and fit for top technological developments and ready to lead disruptive innovations. The experience gained in MobilePass will lead to higher quality proposals in future research.

Mobile Pass also paved the way for several novel and highly innovative research projects on a national and on an international (EU) level.

The EUBAM (EU Border Assistance Mission to Moldova and Ukraine) contacted MobilePass for further tests of a Mobile Solution at the green border (also in trains) of Romania to Ukraine and Moldavia. The Head of Field Operations/Operations Office, EUBAM explicitly expressed his willingness to support future projects on the base of MobilePass, they are interested for a small pilot for mobile identity check

1.9.4 Impact on standardisation

To fulfil these aims, MobilePass project worked with various groups and committees (e.g. such as standardization organization like ICAO, CEN, ISO) through formal and informal mechanisms.

MobilePass was active in standardisation group, CEN TC 224 (Technical Committee), WG 18 (Working Group), 9 member states are represented today in this group: Austria, France, Germany, Italy, Norway, Finland, Spain, Switzerland, UK and EU Organisation Frontex.

The TC 224 deals with “Personal identification and related personal devices with secure element, systems, operations and privacy in a milti sectoral environment”. The WG 18 within TC224 deals with “Biometric application profiles for law enforcement and border control authorities using portable identification systems”.

MobilePass influenced ISO/IEC JTC1 SC17 and SC37 (Subcommittees) in the following ways:

SC17 WG3: This is the working group on Machine Readable Travel Documents (MRTD) which in few words are the passports. We have followed all recommendations from ICAO 9303 and been aware if any important change is to be started in WG3.

SC17 WG11: This working group is in charge of the biometric verification in identification cards.

SC37 WG2: Finally all 3 first parts of 30106 (Object Oriented BioAPI) have been published. Therefore, a future version this standard can be part of the programming inside the MobilePass device.

SC37 WG5: The relationship between this project and this WG, is dealing with how to evaluate the results of the project. 19795 family of standards has been used as a baseline. Also, the impact on environmental conditions (29197) has been considered, as the use of MobilePass in open environments is needed. Finally, as usability analysis has also been carried out, this has supported the work of starting a new standard on the impact of the user interaction on biometric systems. Such a new work item is expected to be approved before July 2017.

1.9.5 Proposal for a new working item (NWIP):

After MobilePass presentation and discussions in the WG18 a new topic was raised: what should be the minimum information given to the border guards? It was not clear and a whole bunch of questions had been raised. The topic was formulated with “Border Check Minimal Information Display”.

MobilePass did a proposal to contribute (also editing) for an emerging TS (Technical Specification). It is expected that the acceptance of a NWIP will be accepted in one of the next CEN TC224/WG18 meetings.

This technical specification focuses on minimum information displayed on devices used in the context of border control and law enforcement. The recommendations given here describe necessary representational visual information elements with a high associative rate between representation and function for smooth exchange of law enforcement agencies personal and equipment.

The need for joint operations on European borders and field operations where identity and permissions have to be checked requires deployment and exchange of border guards and law enforcement officers in different countries. To mitigate the effort in terms of training, handling and familiarization the usage of same/similar data representation on applied devices is recommended.

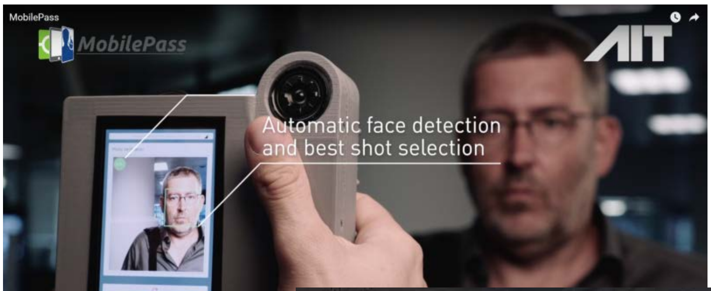
This technical specification covers minimum graphic and contextual data necessary for law enforcement agencies to perform identity and permissions check.

Enrolment, applied technology, device security and integrity as well as capturing methods are out of scope of this new NWIP document.

1.10 Dissemination activities

1.10.1 Summary of publications, media events, scientific papers, workshops and standardisation meetings

- 14 scientific papers submitted to peer-reviewed international conferences
- 1 scientific journal papers submitted to peer-reviewed journals
- 3 scientific conference presentations (panel discussions), with a scope on MobilePass project results
- 24 technical workshop presentations
- 6 trade fair presentations
- 13 standardization committees meetings and discussion attendances
- 4 Videos
  - Project start teaser
  - Technical demo
  - Demonstration Sculeni in TV
  - Living standards award

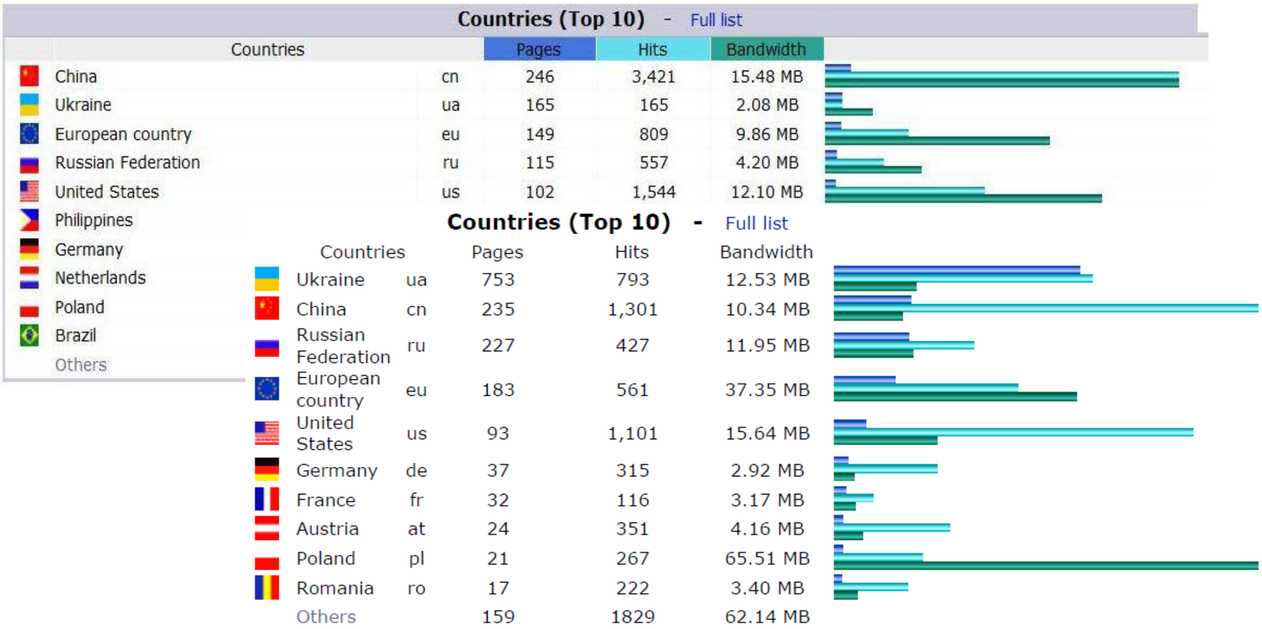


Austrian Standards: Living Standards Awards 2017 - MobilePass – AIT

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

1.10.2 *Website & newspapers*

The MobilePass website - http://www.mobilepass-project.eu/ - has been created in April 2014 and put online upon the start of the project in May 2014. This platform provides key information regarding the project like the objectives, the composition and the dissemination activities of the Consortium or the relevant facts and news linked to the project. This webpage is one of the most important communication channels with the public at large and is therefore regularly updated. The visibility of the webpage has considerably improved along the course of the project with increasing hits.

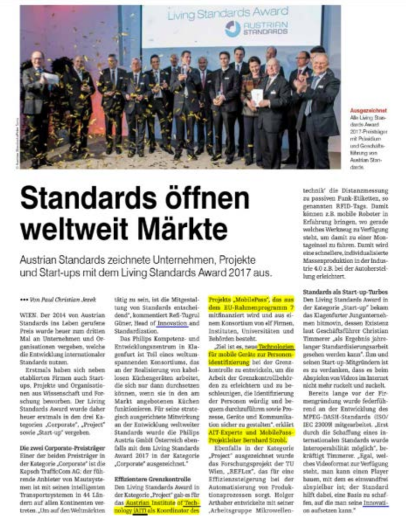


Countries (Top 10) - Full list

Countries		Pages	Hits	Bandwidth
China	cn	246	3,421	15.48 MB
Ukraine	ua	165	165	2.08 MB
European country	eu	149	809	9.86 MB
Russian Federation	ru	115	557	4.20 MB
United States	us	102	1,544	12.10 MB
Philippines				
Germany				
Netherlands				
Poland				
Brazil				
Others				

Countries (Top 10) - Full list

Countries		Pages	Hits	Bandwidth
Ukraine	ua	753	793	12.53 MB
China	cn	235	1,301	10.34 MB
Russian Federation	ru	227	427	11.95 MB
European country	eu	183	561	37.35 MB
United States	us	93	1,101	15.64 MB
Germany	de	37	315	2.92 MB
France	fr	32	116	3.17 MB
Austria	at	24	351	4.16 MB
Poland	pl	21	267	65.51 MB
Romania	ro	17	222	3.40 MB
Others		159	1829	62.14 MB


Living Standards Award
AUSTRIAN STANDARDS

Ausgezeichnet
Alle Living Standards Award 2017-Preisträger mit Präsidium und Geschäftsführung von Austrian Standards.

Standards öffnen weltweit Märkte

Austrian Standards zeichnete Unternehmen, Projekte und Start-ups mit dem Living Standards Award 2017 aus.

••• *Von Paul Christian Jezek*

WIEN. Der 2014 von Austrian Standards ins Leben gerufene Preis wurde heuer zum dritten Mal an Unternehmen und Organisationen vergeben, welche die Entwicklung internationaler Standards nutzen.

Erstmals haben sich neben etablierten Firmen auch Start-ups, Projekte und Organisationen aus Wissenschaft und Forschung beworben. Der Living Standards Award wurde daher heuer erstmals in den drei Kategorien „Corporate", „Project" sowie „Start-up" vergeben.

Die zwei Corporate-Preisträger

Einer der beiden Preisträger in der Kategorie „Corporate" ist die Kapsch TrafficCom AG; der führende Anbieter von Mautsystemen ist mit seinen intelligenten Transportsystemen in 44 Ländern auf allen Kontinenten vertreten. „Um auf den Weltmärkten tätig zu sein, ist die Mitgestaltung von Standards entscheidend", kommentiert Refi-Tugrul Güner, Head of Innovation and Standardization.

Das Philips Kompetenz- und Entwicklungszentrum in Klagenfurt ist Teil eines weltumspannenden Konsortiums, das an der Realisierung von kabellosen Küchengeräten arbeitet, die sich nur dann durchsetzen können, wenn sie in den am Markt angebotenen Küchen funktionieren. Für seine strategisch ausgerichtete Mitwirkung an der Entwicklung weltweiter Standards wurde die Philips Austria GmbH Österreich ebenfalls mit dem Living Standards Award 2017 in der Kategorie „Corporate" ausgezeichnet."

Effizientere Grenzkontrolle

Den Living Standards Award in der Kategorie „Project" gab es für das Austrian Institute of Technology (AIT) als Koordinator des Projekts „MobilePass", das aus dem EU-Rahmenprogramm 7 mitfinanziert wird und aus einem Konsortium von elf Firmen, Instituten, Universitäten und Behörden besteht.

„Ziel ist es, neue Technologien für mobile Geräte zur Personenidentifizierung bei der Grenzkontrolle zu entwickeln, um die Arbeit der Grenzkontrollbehörden zu erleichtern und zu beschleunigen, die Identifizierung der Personen würdig und bequem durchzuführen sowie Prozesse, Geräte und Kommunikation sicher zu gestalten", erklärt AIT-Experte und MobilePass-Projektleiter Bernhard Strobl.

Ebenfalls in der Kategorie „Project" ausgezeichnet wurde das Forschungsprojekt der TU Wien, „REFLex", das für eine Effizienzsteigerung bei der Automatisierung von Produktionsprozessen sorgt. Holger Arthaber entwickelte mit seiner ‚Arbeitsgruppe Mikrowellentechnik' die Distanzmessung zu passiven Funk-Etiketten, so genannten RFID-Tags. Damit können z.B. mobile Roboter in Erfahrung bringen, wo gerade welches Werkzeug zu Verfügung steht, um damit zu einer Montageinsel zu fahren. Damit wird eine schnellere, individualisierte Massenproduktion in der Industrie 4.0 z.B. bei der Autoherstellung erleichtert.

Standards als Start-up-Turbos

Den Living Standards Award in der Kategorie „Start-up" bekam das Klagenfurter Jungunternehmen bitmovin, dessen Existenz laut Geschäftsführer Christian Timmerer „als Ergebnis jahrelanger Standardisierungsarbeit gesehen werden kann". Ihm und seinen Start-up-Mitgründern ist es zu verdanken, dass es beim Abspielen von Videos im Internet nicht mehr ruckelt und zuckelt.

Bereits lange vor der Firmengründung wurde federführend an der Entwicklung des MPEG-DASH-Standards (ISO/IEC 23009) mitgearbeitet. „Erst durch die Schaffung eines internationalen Standards wurde Interoperabilität möglich", bekräftigt Timmerer. „Egal, welches Videoformat zur Verfügung steht, man kann einen Player bauen, mit dem es einwandfrei abspielbar ist; der Standard hilft dabei, eine Basis zu schaffen, auf die man seine Innovation aufsetzen kann."

MobilePass
MobilePass Newsletter #1 July 2015

About MobilePass

MobilePass will focus on research and development towards technologically advanced mobile equipment at land border crossing points. This will allow border control authorities to check European, visa-holding and frequent third country travellers in a comfortable, fast and secure way. The mobile solution incorporates new technologies needed in mobile scenarios and embeds them in the actual border crossing workflow to speed up control procedures.

MobilePass brings together system- and component producers, research institutions and governmental authorities. The entire innovation process, from components development to the integration into an efficient workflow will continuously be evaluated by border guard authorities.

Facts

Project start: **01.05.2014**
Project duration: **30 Months**
Funding: **EU FP7 Security**
Coordinator: **AIT Austrian Institute of Technology**
Consortium: **11 Partners**
Contact: MobilePassCoordinator@ait.ac.at

Visit our WEBSITE for further information.

Optical variable device fullpage Passport scanner
Fast face verification camera
Contactless multiple fingerprint camera
Information systems
© by the MobilePass consortium

• cooperative and fast face capturing and verification

The consortium will develop electronics and algorithms embedded in a trusted platform module with secure boot mechanisms and remote attestation capabilities.

Data Protection within the project:

A major importance is given to privacy and Data Protection concerns within MobilePass. All the research work is compliant with the national and european confidentiality requirements. The Consortium also designed a Consent Form for the biometric and passport data collection, that the volunteers will have to fill in during the upcoming testing phases of the project.

MobilePass
MobilePass Newsletter #2 March 2016

MobilePass passes first review without flaws

The EU funded project MobilePass (Grant No 608016) successfully passed review in December 2015. During the review preliminary demonstrations of technologies took place, like demonstration of a mobile full page passport and document scanner and the demonstration of capturing fingerprints in a contactless way. The preliminary hardware and software for an integrated mobile Device was also shown, paving the way to a prototype in April 2016. All deliverables were accepted. The commission's recommendation was to address more end users and show them the innovations – so we do now with this newsletter !

MobilePass' prototype hardware is in production

According to the Work plan the last steps for miniaturising the preliminary hardware had been done. The preliminary hardware was an intermediate step for the consortium partners to go on with developments before final hardware was available. Now, MobilePass reached the state for setting up the real prototype.

Figure 1: actual 3D drawing of integrated elements (left) and 3D rendering of device (right) - © MobilePass Consortium

MobilePass starts into integration phase

During the last year the consortiums partners had been very busy with their own developments but the time where things have to be put together. First all independently developed modules are integrated into the novel developed MobilePass Device, then afterwards, the Device the Passport Reader, the workflow system and the backend systems are integrated for the mobile and distributed solution.

AIT
Partners devlop individual modules
Platform provided for Partners
Modules are integrated into device
Mobile Solution for Border Guard

Figure 2: modules integration into MobilePass device - © MobilePass Consortium

Figure 3: system integration for solution - © MobilePass Consortium

MobilePass Partners

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

1.10.3 Events/Trades/Fairs

Mobile Pass partners have attended and presented their products and systems at a variety of exhibitions through different events. Exhibition is probably the most direct way to disseminate the results and outcomes to the public, in which case people cannot only see the real products, but also try the technology out people to understand the concept and technology. MobilePass partners have presented at 7 exhibitions across Europe and also in Abu Dhabi at IDEX

- Security Trade Fair Essen
- Security Trade Fair, Essen / Germany 2014
- AVSS Conference Industrial Surveillance Day (Expo)
- GPEC Trade Fair 2016
- Security Trade Fair Essen 2016/09/21
- VISION Trade Fair Stuttgart, Germany 2016/08/11
- IDEX 2017

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

1.11 Exploitation of results

1.11.1 Exploitable Material

Videmo	Fast face recognition algorithms for embedded architectures
	Evaluation results in realistic scenario
AIT	Powerful embedded & secure HW platform
	Development toolchain (PC and embedded)
	Embedded camera driver
	Embedded Security mechanisms
	ARGOS Adapter Client
	Qt Framework (PC and embedded)
Fraunhofer	Image Enhancement Algorithms (e.g. best shot analysis)
	Experience on embedded solutions for image and video processing (e.g. fingerprint capturing as proof of concept)
	Face image reconstruction for forensics (3D face analysis)
	Qt user interface design on embedded platforms
ÎTTI	IDS system and algorithms, also on embedded HW
	Communication switcher
Veridos	Workflow system with full Integration of mobile reader
	Software adapter for an handheld device set with lean communication
INDRA	BSI conform certificates exchange SW
REGULA	Full Showcase and improved communication SW for certificates exchange
UC3M	Methodology for evaluation of biometrics in mobile devices
	Methodology for evaluation of user interaction in biometrics
	Quality checking of fingerprints for interoperability

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608016

1.11.2 Exploitation

Videmo	Face recognition running on tablets in context of elderly care project
	Negotiations with companies in the security domain for access control on embedded devices
AIT	Discussion with Industry for MobilePass Device commercialisation
	Discussion with payment service provider for contactless 4 fingerprint payment - as 2nd factor
	Hardware used in other combination for stereo depth image calculation
	Development contract for vein recognition prototype
	Offer for company (video transmission & enrichment) with similar hardware
	Negotiation phase with company for conceptual phase for embedded stereo
Fraunhofer	Face image reconstruction for police forces (forensic image and video analysis)
	Discussions with several police forces in Germany
	Negotiation with a video management provider (company)
	video processing on embedded platforms for industrial applications
	security applications (traffic monitoring and urban surveillance with low power devices)
	Image enhancement and automated low-quality image detection for time-critical surveillance applications (UAV video exploitation)
ÎTTI	Switching technology used for a mobile network operator
	Negotiations for using switching algorithms in railway applications communication switcher
Veridos	Improved workflow system sold in northern africa
	Negotiations with companies for mobile id verification
INDRA	Negotiations for future exploitation (BSI Frontend)
REGULA	Negotiations with border guards for advanced mobile fullpage passport scanner
UC3M	Methodology for evaluation of biometrics in mobile devices
	Methodology for evaluation of user interaction in biometrics
	Quality checking of fingerprints for interoperability